The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Apache -- Open For Business Project	Cross-site scripting (XSS) vulnerability in ecommerce/control/keywordsearch in the Apache Open For Business Project (OFBiz) allows remote attackers to inject arbitrary web script or HTML via the SEARCH_STRING parameter, a different issue than CVE-2006-6587.	unknown 2006-12-15	7.0	CVE-2006-6589 OTHER-REF
Brian Drawert -- yaplap	PHP remote file inclusion vulnerability in ldap.php in Brian Drawert Yet Another PHP LDAP Admin Project (yaplap) 0.6 and 0.6.1 allows remote attackers to execute arbitrary PHP code via a URL in the LOGIN_style parameter.	unknown 2006-12-15	7.0	CVE-2006-6575 Milw0rm XF
CalaCode -- @mail Webmail System	Cross-site scripting (XSS) vulnerability in @Mail WebMail allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: This information is based upon a vague initial disclosure. Details will be updated after the grace period has ended.	unknown 2006-12-22	7.0	CVE-2006-6700 OTHER-REF SECUNIA
Carsen Klock -- TextSend	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Carsen Klock TextSend 1.5 allow remote attackers to inject arbitrary web script or HTML via the (1) error or (2) success parameter. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-21	7.0	CVE-2006-6695 FRSIRT
chetcpasswd -- chetcpasswd	Pedro Lineu Orso chetcpasswd before 2.4 relies on the X-Forwarded-For HTTP header when verifying a client's status on an IP address ACL, which allows remote attackers to gain unauthorized access by spoofing this header.	unknown 2006-12-21	7.0	CVE-2006-6679 BUGTRAQ OTHER-REF OTHER-REF BID OSVDB SECUNIA XF
chetcpasswd -- chetcpasswd	Pedro Lineu Orso chetcpasswd 2.3.3 does not have a rate limit for client requests, which might allow remote attackers to determine passwords via a dictionary attack.	unknown 2006-12-21	7.0	CVE-2006-6681 BUGTRAQ OTHER-REF

				BID SECUNIA XF
chetcpasswd -- chetcpasswd	Heap-based buffer overflow in Pedro Lineu Orso chetcpasswd before 2.4 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a long X-Forwarded-For HTTP header. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-21	7.0	CVE-2006-6684 OTHER-REF OSVDB SECUNIA
chetcpasswd -- chetcpasswd	Heap-based buffer overflow in Pedro Lineu Orso chetcpasswd 2.3.3 allows local users to cause a denial of service (application crash) and possibly execute arbitrary code via a long REMOTE_ADDR environment variable. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-21	7.0	CVE-2006-6685 SECUNIA
Contra Haber Sistemi -- Contra Haber Sistemi	SQL injection vulnerability in haber.asp in Contra Haber Sistemi 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-12-19	7.0	CVE-2006-6642 BUGTRAQ BID FRSIRT XF
Drupal -- Drupal Project Issue Tracking Drupal -- Drupal Project	Multiple cross-site scripting (XSS) vulnerabilities in Drupal (1) Project Issue Tracking 4.7.x-1.0 and 4.7.x-2.0, and (2) Project 4.6.x-1.0, 4.7.x-1.0, and 4.7.x-2.0 allow remote attackers to inject arbitrary web script or HTML via unspecified parameters, which do not use the check_plain function.	unknown 2006-12-19	7.0	CVE-2006-6646 OTHER-REF FRSIRT SECUNIA BID
Drupal -- Drupal MySite	Cross-site scripting (XSS) vulnerability in the MySite 4.7.x before 4.7.x-3.3 and 5.x before 5.x-1.3 module for Drupal allows remote attackers to inject arbitrary web script or HTML via the Title field when editing a page. NOTE: some details were obtained from third party information.	unknown 2006-12-19	7.0	CVE-2006-6647 OTHER-REF FRSIRT SECUNIA
DWS Systems Inc. -- SQL-Ledger	Unspecified vulnerability in login.pl in SQL Ledger before 2.6.21 allows remote attackers to execute arbitrary Perl code via unknown manipulations of a script variable.	unknown 2006-12-17	7.0	CVE-2006-5872 DEBIAN BID FRSIRT SECTRACK SECUNIA SECUNIA
Eset Software -- NOD32 Antivirus	Integer overflow in ESET NOD32 Antivirus before 1.1743 allows remote attackers to execute arbitrary code via a crafted .DOC file that triggers a heap-based buffer overflow.	unknown 2006-12-20	10.0	CVE-2006-6676 BUGTRAQ OTHER-REF BID FRSIRT
EXlor -- EXlor	PHP remote file inclusion vulnerability in fonctions/template.php in EXlor 1.0 allows remote attackers to execute arbitrary PHP code via a URL in the repphp parameter.	unknown 2006-12-15	7.0	CVE-2006-6591 BUGTRAQ XF
HyperVM -- HyperVM	Cross-site scripting (XSS) vulnerability in display.php in HyperVM 1.2 and earlier allows remote attackers to inject arbitrary web script or HTML via an encoded frm_action parameter. NOTE: the vendor disputes this issue, but it is not certain whether the dispute is about the severity of the issue, or its existence.	unknown 2006-12-19	7.0	CVE-2006-6649 BUGTRAQ OTHER-REF MLIST FRSIRT SECUNIA
Ibiblio -- Osprey	PHP remote file inclusion vulnerability in ListRecords.php in osprey 1.0 allows remote attackers to execute arbitrary PHP code via a URL in the lib_dir parameter.	unknown 2006-12-18	7.0	CVE-2006-6630 BUGTRAQ

JumbaCMS -- JumbaCMS	PHP remote file inclusion vulnerability in includes/functions.php in JumbaCMS 0.0.1 allows remote attackers to execute arbitrary PHP code via a URL in the jcms_root_path parameter.	unknown 2006-12-18	7.0	CVE-2006-6635 Milw0rm BID XF
KMiNT21 Software -- Golden FTP Server	Heap-based buffer overflow in Golden FTP Server (goldenftpd) 1.92 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a long PASS command. NOTE: the USER vector is already covered by CVE-2005-0634.	unknown 2006-12-15	7.0	CVE-2006-6576 OTHER-REF FRSIRT SECUNIA
Linux -- Linux kernel	Multiple buffer overflows in the cmtp_recv_interopmsg function in the Bluetooth driver (net/bluetooth/cmtp/capi.c) in the Linux kernel 2.4.22 up to 2.4.33.4 and 2.6.2 before 2.6.18.6, and 2.6.19.x, allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via CAPI messages with a large value for the length of the (1) manu (manufacturer) or (2) serial (serial number) field.	unknown 2006-12-19	7.0	CVE-2006-6106 MLIST OTHER-REF OTHER-REF FRSIRT SECUNIA SECUNIA XF MLIST
MailEnable -- MailEnable Professional MailEnable -- MailEnable Enterprise MailEnable -- MailEnable Standard	Stack-based buffer overflow in the POP service in MailEnable Standard 1.98 and earlier; Professional 1.84, and 2.35 and earlier; and Enterprise 1.41, and 2.35 and earlier before ME-10026 allows remote attackers to execute arbitrary code via a long argument to the PASS command.	2006-12-18 2006-12-19	7.0	CVE-2006-6605 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECUNIA SECTRACK
Mambo -- ExtCalThai Module	Multiple PHP remote file inclusion vulnerabilities in the ExtCalThai (com_extcalendar) 0.9.1 and earlier component for Mambo allow remote attackers to execute arbitrary PHP code via a URL in (1) the CONFIG_EXT[LANGUAGES_DIR] parameter to admin_events.php, (2) the mosConfig_absolute_path parameter to extcalendar.php, or (3) the CONFIG_EXT[LIB_DIR] parameter to lib/mail.inc.php.	unknown 2006-12-18	7.0	CVE-2006-6634 BUGTRAQ BID XF
MaxiASP -- Burak Yilmaz Download Portal	SQL injection vulnerability in down.asp in Burak Yylmaz Download Portal allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-12-20	7.0	CVE-2006-6671 BUGTRAQ BID FRSIRT SECUNIA
MaxiASP -- Burak Yilmaz Download Portal	Multiple SQL injection vulnerabilities in Burak Yylmaz Download Portal allow remote attackers to execute arbitrary SQL commands via the (1) kid or possibly (2) id parameter to (a) HABERLER.ASP and (b) ASPKAT.ASP. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-20	7.0	CVE-2006-6672 FRSIRT
Microsoft -- IIS	Microsoft Internet Information Services (IIS) 5.1 permits the IUSR_Machine account to execute non-EXE files such as .COM files, which allows attackers to execute arbitrary commands via arguments to any .COM file that executes those arguments, as demonstrated using win.com when it is in a web directory with certain permissions.	unknown 2006-12-15	7.0	CVE-2006-6578 BUGTRAQ
Moodle -- Moodle	Cross-site scripting (XSS) vulnerability in an unspecified component of Moodle 1.5 allows remote attackers to inject arbitrary web script or HTML via a javascript URI in the SRC attribute of an IMG element. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information. NOTE: It is unclear whether this candidate	unknown 2006-12-18	7.0	CVE-2006-6626 OTHER-REF BID

	overlaps CVE-2006-4784 or CVE-2006-4941.			
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Multiple unspecified vulnerabilities in the layout engine for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via unknown impact and attack vectors.	unknown 2006-12-19	7.0	CVE-2006-6497 OTHER-REF REDHAT REDHAT REDHAT SECTRACK SECTRACK SECTRACK SECUNIA SECUNIA SECUNIA
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Multiple unspecified vulnerabilities in the JavaScript engine for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via unknown impact and attack vectors.	unknown 2006-12-19	7.0	CVE-2006-6498 OTHER-REF REDHAT REDHAT REDHAT SECTRACK SECTRACK SECTRACK SECUNIA SECUNIA SECUNIA
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Heap-based buffer overflow in Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by setting the CSS cursor to certain images that cause an incorrect size calculation when converting to a Windows bitmap.	unknown 2006-12-19	7.0	CVE-2006-6500 OTHER-REF SECTRACK SECTRACK SECTRACK
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Unspecified vulnerability in Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to gain privileges and install malicious code via the watch Javascript function.	unknown 2006-12-19	7.0	CVE-2006-6501 OTHER-REF REDHAT REDHAT REDHAT SECTRACK SECTRACK SECTRACK SECUNIA SECUNIA SECUNIA
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to bypass cross-site scripting (XSS) protection by changing the src attribute of an IMG element to a javascript: URI.	unknown 2006-12-19	7.0	CVE-2006-6503 OTHER-REF REDHAT REDHAT REDHAT SECTRACK SECTRACK SECTRACK SECUNIA SECUNIA SECUNIA
Mozilla -- SeaMonkey Mozilla -- Thunderbird	Multiple heap-based buffer overflows in Mozilla Thunderbird before 1.5.0.9 and SeaMonkey before 1.0.7 allow remote attackers to execute arbitrary code via (1) external message modies with long Content-Type headers or (2) long RFC2047-encoded (MIME non-ASCII) headers.	unknown 2006-12-19	7.0	CVE-2006-6505 OTHER-REF REDHAT REDHAT SECTRACK SECTRACK

				SECUNIA SECUNIA
mxBB -- mxBB Web Links	PHP remote file inclusion vulnerability in language/lang_english/lang_admin.php in the Web Links (mx_links) 2.05 and earlier module for mxBB allows remote attackers to execute arbitrary PHP code via a URL in the mx_root_path parameter.	unknown 2006-12-19	7.0	CVE-2006-6645 OTHER-REF BID FRSIRT XF
Neocrome -- Seditio Neocrome -- Land Down Under	SQL injection vulnerability in polls.php in Neocrome Land Down Under (LDU) 8.x and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-12-15	7.0	CVE-2006-6577 BUGTRAQ BID
Netrik -- Netrik	The edit_textarea function in form-file.c in Netrik 1.15.4 and earlier does not properly verify temporary filenames when editing textarea fields, which allows attackers to execute arbitrary commands via shell metacharacters in the filename.	unknown 2006-12-20	7.0	CVE-2006-6678 OTHER-REF OTHER-REF FRSIRT
Novell -- Novell Apache Novell -- Netware	Cross-site scripting (XSS) vulnerability in Novell NetWare 6.5 Support Pack 5 and 6 and Novell Apache on NetWare 2.0.48 allows remote attackers to inject arbitrary web script or HTML via unspecifeid parameters in Welcome web-app.	unknown 2006-12-20	7.0	CVE-2006-6675 OTHER-REF FRSIRT SECUNIA
Omniture -- SiteCatalyst	Multiple cross-site scripting (XSS) vulnerabilities in Omniture SiteCatalyst allow remote attackers to inject arbitrary web script or HTML via the (1) ss parameter in (a) search.asp and the (2) company and (3) username fields on (b) the web login page. NOTE: some details were obtained from third party information.	unknown 2006-12-19	7.0	CVE-2006-6640 BUGTRAQ BID SECTRACK XF
Oracle -- Portal	CRLF injection vulnerability in webapp/jsp/calendar.jsp in Oracle Portal 10g allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via CRLF sequences in the enc parameter, possibly involving iso-8859-1 encoding.	unknown 2006-12-21	7.0	CVE-2006-6697 BUGTRAQ BUGTRAQ FULLDISC FULLDISC BID
Paristemi -- Paristemi	Multiple PHP remote file inclusion vulnerabilities in Paristemi 0.8.3 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the SERVER_DIRECTORY parameter to unspecified scripts, a different vector than CVE-2006-????. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-21	7.0	CVE-2006-6689 FRSIRT
PHP-Update -- PHP-Update	Variable overwrite vulnerability in blog.php in PHP-Update 2.7 and earlier allows remote attackers to overwrite arbitrary program variables and execute arbitrary PHP code via multiple vectors that use the extract function, as demonstrated by the (1) f, (2) newmessage, (3) newusername, (4) adminuser, and (5) permission parameters.	unknown 2006-12-20	7.0	CVE-2006-6661 OTHER-REF FRSIRT SECUNIA
planetluc.com -- RateMe	PHP remote file inclusion vulnerability in main.inc.php in planetluc.com RateMe 1.3.2 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the pathtoscript parameter.	unknown 2006-12-19	7.0	CVE-2006-6648 BUGTRAQ BID FRSIRT
ScriptMate -- User Manager	Multiple cross-site scripting (XSS) vulnerabilities in ScriptMate User Manager 2.1 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) members_username (user) and (2) members_password (password) fields in a login action in members/default.asp, and (3) the Search box. NOTE: some of these details are obtained from third party information.	unknown 2006-12-15	7.0	CVE-2006-6582 OTHER-REF FRSIRT SECTRACK SECUNIA XF
scriptsfrenzy.com -- E-Uploader Pro	Directory traversal vulnerability in include/config.php in E-Uploader Pro 1.0 and earlier allows remote attackers to execute arbitrary PHP code via a .. (dot dot) in the language parameter, as demonstrated by uploading a .JPG file containing PHP code, then	unknown 2006-12-21	7.0	CVE-2006-6694 OTHER-REF OTHER-REF BID

	accessing the file via config.php.			SECUNIA XF
Softwin -- BitDefender Softwin -- BitDefender Antivirus Softwin -- BitDefender Online Scanner Softwin -- BitDefender Internet Security Softwin -- BitDefender Mail Protection	Integer overflow in the packed PE file parsing implementation in BitDefender products before 20060829, including Antivirus, Antivirus Plus, Internet Security, Mail Protection for Enterprises, and Online Scanner; and BitDefender products for Microsoft ISA Server and Exchange 5.5 through 2003; allows remote attackers to execute arbitrary code via a crafted file, which triggers a heap-based buffer overflow, aka the "cevakrnl.xmd vulnerability."	unknown 2006-12-18	10.0	CVE-2006-6627 BUGTRAQ OTHER-REF BID FULLDISC FRSIRT SECTRACK SECUNIA XF
Typo3 -- Typo3	rtehtmlarea/pi1/class.tx_rtehtmlarea_pi1.php in Typo3 4.0.0 through 4.0.3, 3.7 and 3.8 with the rtehtmlarea extension, and 4.1 beta allows remote authenticated users to execute arbitrary commands via shell metacharacters in the userUid parameter to rtehtmlarea/htmlarea/plugins/SpellChecker/spell-check-logic.php, and possibly another vector.	unknown 2006-12-21	10.0	CVE-2006-6690 BUGTRAQ MLIST MLIST OTHER-REF BID FRSIRT
Unicenter -- Database Management Portal Unicenter -- Database Command Center Unicenter -- Enterprise Job Manager CleverPath -- Portal Unicenter -- Workload Control Center Unicenter -- Asset and Portfolio Management CleverPath -- Aion BPM eTrust -- Security Command Center Unicenter -- Management Portal BrightStor -- Portal CA -- CleverPath Portal	Unspecified vulnerability in CA CleverPath Portal before maintenance version 4.71.001_179_060830, as used in multiple products including BrightStor Portal r11.1, CleverPath Aion BPM r10 through r10.2, eTrust Security Command Center r1 and r8, and Unicenter, does not properly handle when multiple Portal servers are started at the same time and share the same data store, which might cause a Portal user to inherit the session and credentials of a user who is on another Portal server.	unknown 2006-12-19	7.0	CVE-2006-6641 OTHER-REF FRSIRT SECUNIA
Valdersoft -- Shopping Cart	Multiple PHP remote file inclusion vulnerabilities in Valdersoft Shopping Cart 3.0 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the commonIncludePath parameter to (1) admin/include/common.php, (2) include/common.php, or (3) common_include/common.php.	unknown 2006-12-21	7.0	CVE-2006-6691 OTHER-REF BID FRSIRT XF
VerliAdmin -- VerliAdmin	PHP remote file inclusion vulnerability in index.php in VerliAdmin 0.3 and earlier allows remote authenticated users to execute arbitrary PHP code via a URL in the q parameter.	unknown 2006-12-20	7.0	CVE-2006-6666 OTHER-REF BID FRSIRT SECUNIA

VerliAdmin -- VerliAdmin	Multiple SQL injection vulnerabilities in VerliAdmin 0.3 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) nick_mod or (2) nick parameter to (a) repass.php or (b) verify.php. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-20	7.0	CVE-2006-6667 FRSIRT
VerliAdmin -- VerliAdmin	Cross-site scripting (XSS) vulnerability in VerliAdmin 0.3 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-20	7.0	CVE-2006-6668 FRSIRT
Vernet Loic -- PHP_Debug	PHP remote file inclusion vulnerability in tests/debug_test.php in Vernet Loic PHP_Debug 1.1.0 allows remote attackers to execute arbitrary PHP code via a URL in the debugClassLocation parameter.	unknown 2006-12-15	7.0	CVE-2006-6581 BUGTRAQ BID SECTRACK XF
Web-APP.net -- Web-APP.net Web-APP.org -- Web-APP.org	Web Automated Perl Portal (WebAPP) 0.9.9.4, and 0.9.9.3.4 Network Edition (NE) (aka WebAPP.NET) allows remote attackers to bypass filtering mechanisms via unknown vectors. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-21	7.0	CVE-2006-6688 BID
WebAPP -- WebAPP Network Edition WebAPP -- WebAPP	Cross-site scripting (XSS) vulnerability in Web Automated Perl Portal (WebAPP) 0.9.9.4, and 0.9.9.3.4 Network Edition (NE) (aka WebAPP.NET), allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-21	7.0	CVE-2006-6687 BID
WebCalendar -- WebCalendar	Cross-site scripting (XSS) vulnerability in export_handler.php in WebCalendar 1.0.4 and earlier allows remote attackers to inject arbitrary web script or HTML via the format parameter.	unknown 2006-12-20	7.0	CVE-2006-6669 SECUNIA BUGTRAQ FRSIRT
WeBWorK -- Program Generation Language	lib/WeBWorK/PG/Translator.pm in WeBWorK Program Generation (PG) Language before 2.3.1 uses an insufficiently restrictive regular expression to determine valid macro filenames, which allows attackers to load arbitrary macro files whose names contain the strings (1) dangerousMacros.pl, (2) PG.pl, or (3) IO.pl.	unknown 2006-12-18	7.0	CVE-2006-6629 OTHER-REF BID FRSIRT
Yahoo! -- Yahoo! Messenger	Buffer overflow in the YMMAPI.YMailAttach ActiveX control (ymmapi.dll) before 2005.1.1.4 in Yahoo! Messenger allows remote attackers to execute arbitrary code via a crafted HTML document. NOTE: some details were obtained from third party information.	unknown 2006-12-15	10.0	CVE-2006-6603 OTHER-REF FRSIRT SECUNIA CERT-VN BID SECTRACK
YapBB -- YapBB	PHP remote file inclusion vulnerability in include/yapbb_session.php in YapBB 1.2 Beta2 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the GLOBALS[include_Bit] parameter.	unknown 2006-12-18	7.0	CVE-2006-6633 Milw0rm BID XF
ZABBIX -- ZABBIX	Multiple format string vulnerabilities in zabbix before 20061006 allow attackers to cause a denial of service (application crash) and possibly execute arbitrary code via format string specifiers in information that would be recorded in the system log using (1) zabbix_log or (2) zabbix_syslog.	unknown 2006-12-21	7.0	CVE-2006-6692 OTHER-REF OTHER-REF BID FRSIRT SECUNIA

ZABBIX -- ZABBIX	Multiple buffer overflows in zabbix before 20061006 allow attackers to cause a denial of service (application crash) and possibly execute arbitrary code via long strings to the (1) zabbix_log and (2) zabbix_syslog functions.	unknown 2006-12-21	7.0	CVE-2006-6693 OTHER-REF OTHER-REF BID FRSIRT SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Astonsoft -- DeepBurner Pro Astonsoft -- DeepBurner Free	Buffer overflow in Astonsoft DeepBurner Pro and Free 1.8.0 and earlier allows user-assisted remote attackers to execute arbitrary code via a long file name tag in a dbr file.	unknown 2006-12-20	5.6	CVE-2006-6665 OTHER-REF FRSIRT
chetcpasswd -- chetcpasswd	Multiple unspecified vulnerabilities in chetcpasswd 2.4.1 allow local users to gain privileges via unspecified vectors related to executing (1) the cp program, (2) the mail program, or (3) the program specified in the post_change configuration line.	unknown 2006-12-19	4.9	CVE-2006-6639 BID SECUNIA
chetcpasswd -- chetcpasswd	Pedro Lineu Orso chetcpasswd before 2.3.1 does not document the need for 0400 permissions on /etc/chetcpasswd.allow, which might allow local users to gain sensitive information by reading this file.	unknown 2006-12-21	4.9	CVE-2006-6680 OTHER-REF
Genepi -- Genepi	PHP remote file inclusion vulnerability in genepi.php in Genepi 1.6 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the topdir parameter.	unknown 2006-12-18	5.6	CVE-2006-6632 Milw0rm BID XF
Ibiblio -- Osprey	PHP remote file inclusion vulnerability in lib/xml/oai/GetRecord.php in osprey 1.0 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the lib_dir parameter.	unknown 2006-12-18	5.6	CVE-2006-6631 Milw0rm BID XF
IBM -- Websphere Application Server	Unspecified vulnerability in the Utility Classes for IBM WebSphere Application Server (WAS) before 5.1.1.13 and 6.x before 6.0.2.17 has unknown impact and attack vectors.	unknown 2006-12-19	4.9	CVE-2006-6636 OTHER-REF OTHER-REF AIXAPAR BID FRSIRT SECUNIA SECUNIA BID FRSIRT XF
Intel -- 2200BG PROSet/Wireless	Race condition in W29N51.SYS in the Intel 2200BG wireless driver 9.0.3.9 allows remote attackers to cause memory corruption and execute arbitrary code via a series of crafted beacon frames. NOTE: some details are obtained solely from third party information.	unknown 2006-12-19	5.6	CVE-2006-6651 OTHER-REF BID FRSIRT SECUNIA
Moodle -- Moodle	Cross-site scripting (XSS) vulnerability in mod/forum/discuss.php in Moodle 1.6.1 allows remote attackers to inject arbitrary web script or HTML via the navtail parameter. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-18	5.6	CVE-2006-6625 OTHER-REF BID

mxBB -- mxBB Meeting	PHP remote file inclusion vulnerability in pages/meeting_constants.php in the Meeting (mx_meeting) 1.1.2 and earlier module for mxBB allows remote attackers to execute arbitrary PHP code via a URL in the module_root_path parameter.	unknown 2006-12-19	5.6	CVE-2006-6644 OTHER-REF BID FRSIRT SECUNIA XF
mxBB -- mxBB Charts	PHP remote file inclusion vulnerability in charts_constants.php in the Charts (mx_charts) 1.0.0 and earlier module for mxBB allows remote attackers to execute arbitrary PHP code via a URL in the module_root_path parameter.	unknown 2006-12-19	5.6	CVE-2006-6650 OTHER-REF BID FRSIRT SECUNIA XF
NetBSD -- NetBSD	Buffer overflow in the glob implementation in libc in NetBSD-current before 20050914, and NetBSD 2.* and 3.* before 20061203, as used by the FTP daemon, allows remote authenticated users to execute arbitrary code via a long pathname that results from path expansion.	unknown 2006-12-19	6.0	CVE-2006-6652 NETBSD SECTRACK
Nortel -- CallPilot Server	Unspecified vulnerability in Nortel CallPilot 4.x Server has unknown impact and attack vectors, aka P-2006-0011-GLOBAL.	unknown 2006-12-20	4.9	CVE-2006-6670 OTHER-REF SECUNIA
SCRIPTPHP -- ProNews	admin/change.php in ProNews 1.5 does not check whether a user is permitted to change news items, which allows remote attackers to add or delete information within an item, and possibly have other impacts. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-15	4.7	CVE-2006-6580 SECUNIA
TextSend -- TextSend	PHP remote file inclusion vulnerability in sender.php in Carsen Klock TextSend 1.5 allows remote attackers to execute arbitrary PHP code via a URL in the ROOT_PATH parameter.	unknown 2006-12-21	5.6	CVE-2006-6686 BID FRSIRT

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
	The GConf daemon (gconfd) in GConf 2.14.0 creates temporary files under directories with names based on the username, even when GCONF_GLOBAL_LOCKS is not set, which allows local users to cause a denial of service by creating the directories ahead of time, which prevents other users from using Gnome.	unknown 2006-12-22	1.3	CVE-2006-6698 OTHER-REF OTHER-REF
Apple -- Mac OS X Server Apple -- Mac OS X	QuickTime for Java on Mac OS X 10.4 through 10.4.8, when used with Quartz Composer, allows remote attackers to obtain sensitive information (screen images) via a Java applet that accesses images that are being rendered by other embedded QuickTime objects.	unknown 2006-12-19	1.9	CVE-2006-5681 OTHER-REF APPLE SECTRACK SECUNIA
chetcpasswd -- chetcpasswd	Pedro Lineu Orso chetcpasswd 2.3.3 provides a different error message when a request with a valid username fails, compared to a request with an invalid username, which allows remote attackers to determine valid usernames on the system.	unknown 2006-12-21	2.3	CVE-2006-6682 BUGTRAQ OTHER-REF BID OSVDB SECUNIA XF

chetcpasswd -- chetcpasswd	Pedro Lineu Orso chetcpasswd 2.4.1 and earlier verifies and updates user accounts via custom code that processes /etc/shadow and does not follow the PAM configuration, which might allow remote attackers to bypass intended restrictions implemented through PAM.	unknown 2006-12-21	3.3	CVE-2006-6683 OTHER-REF BID
Eset Software -- NOD32 Antivirus	ESET NOD32 Antivirus before 1.1743 allows remote attackers to cause a denial of service (crash) via a crafted .CHM file that triggers a divide-by-zero error.	unknown 2006-12-20	2.3	CVE-2006-6677 BUGTRAQ OTHER-REF BID FRSIRT
Fightersoft Multimedia -- Star FTP Server	Fightersoft Multimedia Star FTP server 1.10 allows remote attackers to cause a denial of service (crash) via multiple RETR commands with long arguments.	unknown 2006-12-19	3.3	CVE-2006-6643 OTHER-REF BID FRSIRT SECUNIA XF
IBM -- Websphere Application Server	The Servlet Engine and Web Container in IBM WebSphere Application Server (WAS) before 6.0.2.17 allows attackers to read the source code of JSP files and obtain sensitive information via unspecified vectors.	unknown 2006-12-19	1.6	CVE-2006-6637 OTHER-REF AIXAPAR SECUNIA BID FRSIRT
IBM -- DB2 Universal Database	IBM DB2 8.1 before FixPak 14 allows remote attackers to cause a denial of service via a crafted SQLJRA packet, which causes a NULL pointer dereference in the sqle_db2ra_as_recvrequest function in DB2ENGN.DLL, a different issue than CVE-2006-4257.	unknown 2006-12-19	3.3	CVE-2006-6638 OTHER-REF AIXAPAR BID SECUNIA
Inktomi -- Inktomi Search	Inktomi Search 4.1.4 allows remote attackers to obtain sensitive information via direct requests with missing parameters to (1) help/header.html, (2) thesaurus.html, and (3) topics.html, which leak the installation path in the resulting error message, a related issue to CVE-2006-5970.	unknown 2006-12-19	2.3	CVE-2006-6658 SECTRACK
KDE -- libkhtml	The nodeType function in KDE libkhtml 4.2.0 and earlier, as used by Konquerer, KMail, and other programs, allows remote attackers to cause a denial of service (crash) via malformed HTML tags, possibly involving a COL SPAN tag embedded in a RANGE tag.	unknown 2006-12-20	1.9	CVE-2006-6660 OTHER-REF BID FRSIRT
Linux -- Linux kernel	The mincore function in the Linux kernel before 2.4.33.6 does not properly lock access to user space, which has unspecified impact and attack vectors, possibly related to a deadlock.	unknown 2006-12-19	1.0	CVE-2006-4814 OTHER-REF BID FRSIRT SECUNIA
Mandiant -- First Response	FRAgent.exe in Mandiant First Response (MFR) before 1.1.1, when run in daemon mode with SSL enabled, allows remote attackers to cause a denial of service (refused connections) via malformed requests, which results in a mishandled exception.	unknown 2006-12-19	2.7	CVE-2006-6475 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECTRACK SECUNIA
Mandiant -- First Response	FRAgent.exe in Mandiant First Response (MFR) before 1.1.1, when run in daemon mode and when the agent is bound to 0.0.0.0 (all interfaces), opens sockets in non-exclusive mode, which allows local users to hijack the socket, and capture data or cause a denial of service (loss of daemon operation).	unknown 2006-12-19	1.6	CVE-2006-6476 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECTRACK SECUNIA

Mandiant -- First Response	FRAgent.exe in Mandiant First Response (MFR) before 1.1.1, when run in daemon mode and configured to use only HTTP, allows local users to modify requests and responses between a client and an agent by hijacking an HTTP FRAgent daemon and conducting a man-in-the-middle (MITM) attack.	unknown 2006-12-19	1.6	CVE-2006-6477 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECTRACK SECUNIA
Mantis -- Mantis	Mantis before 1.1.0a2 does not implement per-item access control for Issue History (Bug History), which allows remote attackers to obtain sensitive information by reading the Change column, as demonstrated by the Change column of a custom field.	unknown 2006-12-15	2.3	CVE-2006-6574 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF SECUNIA FRSIRT XF
Marathon Aleph One -- Marathon Aleph One	The server component in Marathon Aleph One before 0.17.1 and 2006-12-17 allows remote attackers to cause a denial of service (application crash) via unspecified vectors related to "gathering net games."	unknown 2006-12-20	2.3	CVE-2006-6663 OTHER-REF OTHER-REF OTHER-REF FRSIRT SECUNIA
Marathon Aleph One -- Marathon Aleph One	Format string vulnerability in Marathon Aleph One before 0.17.1 and 2006-12-17 might allow remote attackers to cause a denial of service (application crash) or execute arbitrary code via format string specifiers in the TopLevelLogger::logMessageV function in Misc/Logging.cpp. NOTE: some details were obtained from third party information.	unknown 2006-12-20	2.3	CVE-2006-6664 OTHER-REF OTHER-REF OTHER-REF FRSIRT SECUNIA
Microsoft -- IIS	Microsoft Windows XP has weak permissions (FILE_WRITE_DATA and FILE_READ_DATA for Everyone) for %WINDIR%\pchealth\ERRORREP\QHEADLES, which allows local users to write and read files in this folder, as demonstrated by an ASP shell that has write access by IWAM_machine and read access by IUSR_Machine.	unknown 2006-12-15	3.9	CVE-2006-6579 BUGTRAQ
Microsoft -- Internet Explorer Microsoft -- Windows XP Microsoft -- Outlook	The Microsoft Office Outlook Recipient ActiveX control (ole32.dll) in Windows XP SP2 allows remote attackers to cause a denial of service (Internet Explorer 7 hang) via crafted HTML.	unknown 2006-12-19	2.3	CVE-2006-6659 OTHER-REF BID SECTRACK
Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Windows Vista Microsoft -- Windows XP	Double-free vulnerability in Microsoft Windows 2000, XP, 2003, and Vista allows local users to gain privileges by calling the MessageBox function with a MB_SERVICE_NOTIFICATION message with crafted data, which sends a HardError message to Client/Server Runtime Server Subsystem (CSRSS) process, which is not properly handled when invoking the UserHardError and GetHardErrorText functions in WINSRV.DLL.	unknown 2006-12-21	1.6	CVE-2006-6696 OTHER-REF BID OTHER-REF OTHER-REF OTHER-REF

Mono -- XSP	The System.Web class in the XSP for ASP.NET server 1.1 through 2.0 in Mono does not properly verify local pathnames, which allows remote attackers to (1) read source code by appending a space (%20) to a URI, and (2) read credentials via a request for Web.Config%20.	2006-11-29 2006-12-21	2.3	CVE-2006-6104 BUGTRAQ OTHER-REF MANDRIVA UBUNTU BID FRSIRT SECUNIA SECUNIA SECUNIA
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	The js_dtoa function in Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 overwrites memory instead of exiting when the floating point precision is reduced, which allows remote attackers to cause a denial of service via any plugins that reduce the precision.	unknown 2006-12-19	1.9	CVE-2006-6499 OTHER-REF SECTRACK SECTRACK SECTRACK
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Use-after-free vulnerability in the LiveConnect bridge code for Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, Thunderbird before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to cause a denial of service (crash) via unknown vectors.	unknown 2006-12-19	3.3	CVE-2006-6502 OTHER-REF REDHAT REDHAT REDHAT SECTRACK SECTRACK SECTRACK SECUNIA SECUNIA SECUNIA
Mozilla -- SeaMonkey Mozilla -- Firefox Mozilla -- Thunderbird	Mozilla Firefox 2.x before 2.0.0.1, 1.5.x before 1.5.0.9, and SeaMonkey before 1.0.7 allows remote attackers to cause a denial of service (crash) by appending an SVG comment DOM node to another type of document, which triggers memory corruption.	unknown 2006-12-19	2.3	CVE-2006-6504 OTHER-REF BUGTRAQ OTHER-REF REDHAT REDHAT REDHAT SECTRACK SECTRACK SECUNIA SECUNIA SECUNIA
Mozilla -- Firefox	The "Feed Preview" feature in Mozilla Firefox 2.0 before 2.0.0.1 sends the URL of the feed when requesting favicon.ico icons, which results in a privacy leak that might allow feed viewing services to determine browsing habits.	unknown 2006-12-19	2.3	CVE-2006-6506 OTHER-REF OTHER-REF SECTRACK
Mozilla -- Firefox	Mozilla Firefox 2.0 before 2.0.0.1 allows remote attackers to bypass Cross-Site Scripting (XSS) protection via vectors related to a Function.prototype regression error.	unknown 2006-12-19	2.3	CVE-2006-6507 OTHER-REF SECTRACK
NeoScale Systems -- CryptoStor Tape 700	The NeoScale Systems CryptoStor 700 series appliance before 2.6 relies on client-side ActiveX code for smartcard authentication, which allows remote attackers to bypass smartcard authentication, and gain access if able to present a valid username and password, by disabling ActiveX.	unknown 2006-12-19	3.4	CVE-2006-3896 CERT-VN BID SECUNIA FRSIRT SECTRACK
NetBSD -- NetBSD	The accept function in NetBSD-current before 20061023, NetBSD 3.0 and 3.0.1 before 20061024, and NetBSD 2.x before 20061029 allows local users to cause a denial of service (socket consumption) via an invalid (1) name or (2) namelen parameter, which may result in the socket never being closed (aka "a dangling socket").	unknown 2006-12-19	1.0	CVE-2006-6653 NETBSD SECTRACK

NetBSD -- NetBSD	The sendmsg function in NetBSD-current before 20061023, NetBSD 3.0 and 3.0.1 before 20061024, and NetBSD 2.x before 20061029, when run on a 64-bit architecture, allows attackers to cause a denial of service (kernel panic) via an invalid msg_controllen parameter to the sendit function.	unknown 2006-12-19	1.9	CVE-2006-6654 NETBSD SECTRACK
NetBSD -- NetBSD	The procfs implementation in NetBSD-current before 20061023, NetBSD 3.0 and 3.0.1 before 20061024, and NetBSD 2.x before 20061029 allows local users to cause a denial of service (kernel panic) by attempting to access /emul/linux/proc/0/stat on a procfs filesystem that was mounted with mount_procfs -o linux, which results in a NULL pointer dereference.	unknown 2006-12-19	1.0	CVE-2006-6655 NETBSD SECTRACK
NetBSD -- NetBSD	Unspecified vulnerability in ptrace in NetBSD-current before 20061027, NetBSD 3.0 and 3.0.1 before 20061027, and NetBSD 2.x before 20061119 allows local users to read kernel memory and obtain sensitive information via certain manipulations of a PT_LWPINFO request, which leads to a memory leak and information leak.	unknown 2006-12-19	1.6	CVE-2006-6656 NETBSD SECTRACK
NetBSD -- NetBSD	The if_clone_list function in NetBSD-current before 20061027, NetBSD 3.0 and 3.0.1 before 20061027, and NetBSD 2.x before 20061119 allows local users to read potentially sensitive, uninitialized stack memory via unspecified vectors.	unknown 2006-12-19	1.6	CVE-2006-6657 NETBSD SECTRACK
OpenOffice -- OpenOffice	Integer overflow in OpenOffice.org (OOo) 2.1 allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted DOC file, as demonstrated by the 12122006-djtest.doc file, a variant of CVE-2006-6561 in a separate codebase.	unknown 2006-12-18	1.9	CVE-2006-6628 BUGTRAQ BUGTRAQ Milw0rm Milw0rm BID FRSIRT
Oracle -- Portal	Multiple CRLF injection vulnerabilities in Oracle Portal 9.0.2 and possibly other versions allow remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via CRLF sequences in the enc parameter to (1) calendarDialog.jsp or (2) fred.jsp. NOTE: the calendar.jsp vector is covered by CVE-2006-6697.	unknown 2006-12-22	2.3	CVE-2006-6699 BUGTRAQ
Ozeki -- HTTP-SMS Gateway	Ozeki HTTP-SMS Gateway 1.0, and possibly earlier, stores usernames and passwords in plaintext in theHKLM\Software\Ozeki\SMSServer\CurrentVersion\Plugins\httpsmsgate registry key, which allows local users to obtain sensitive information. NOTE: The provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-12-20	1.6	CVE-2006-6674 SECUNIA
SuSE -- SuSE Open Enterprise Server SuSE -- SuSE Linux Enterprise Desktop	Unspecified vulnerability in Linux User Management (novell-lum) on SUSE Linux Enterprise Desktop 10 and Open Enterprise Server 9, under unspecified conditions, allows local users to log in to the console without a empty password.	unknown 2006-12-20	2.3	CVE-2006-6662 SUSE SECUNIA
Windows -- Media Player Microsoft -- Windows XP	Windows Media Player 10.00.00.4036 in Microsoft Windows XP SP2 allows user-assisted remote attackers to cause a denial of service via a .MID (MIDI) file with a malformed header chunk without any track chunks, possibly involving (1) number of tracks of (2) time division fields that are set to 0.	unknown 2006-12-15	1.9	CVE-2006-6601 BUGTRAQ MLIST BID FRSIRT
WinFTP Server -- WinFTP Server	WinFtp Server 2.0.2 allows remote attackers to cause a denial of service (crash) via long (1) PASV, (2) LIST, (3) USER, (4) PORT, and possibly other commands.	unknown 2006-12-20	2.3	CVE-2006-6673 OTHER-REF FRSIRT SECUNIA

Back to top